International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 3 1728 - 1732

Secure Cloud Computing Based On Mobile Agents

Sanjivanee R. Kale
M.E.Scholar,
Department of Computer Sci. & Engg
P.R.PATIL COE&T,Amravati.
Sanjivanikale5998@gmail.com

Prof P. D. Soni
Assistant Professor,
Department of Computer Sci. & Engg.
P.R.PATIL COE&T,Amravati.
pravindsoni@gmail.com

Abstract:- In this paper, we provide protection to the service requested to the cloud from user. Cloud computing is a examine sloping system that launch services to the client at low cost. According to various researches user verification is the most significant security concern and demanding issue in cloud-based environment. As cloud computing provides different advantages it also brings some of the concern about the security and privacy of information.
Cloud computing requests to concentrate on three main security issues : privacy, reliability and accessibility. In this paper, we propose a new approach that provides confidentiality for the services request by the user by using mobile agents for communication between user and cloud layer; we provide security at each layer in cloud computing with Kerberos. We provide security to service which will be request to the cloud with authentication server and TGS system.

Index Words- *Multi-agent System, Mobile agent, cloud computing, AS (Authentication Server), TGS*

*****

I. Introduction

The Cloud computing essentially supplies all applications and databases in the data center which are placed at different location. Cloud Computing provides Internet-based services, computing, and storage for users in all markets together with economic , healthcare, and administration and those essential computing infrastructure is used only when it is needed. In cloud computing, resources are provided as a service over the Internet to customers who use them.

We distinguish three types of cloud computing: the public cloud, private cloud and hybrid cloud is actually a combination the first two (Figure 1)[1].

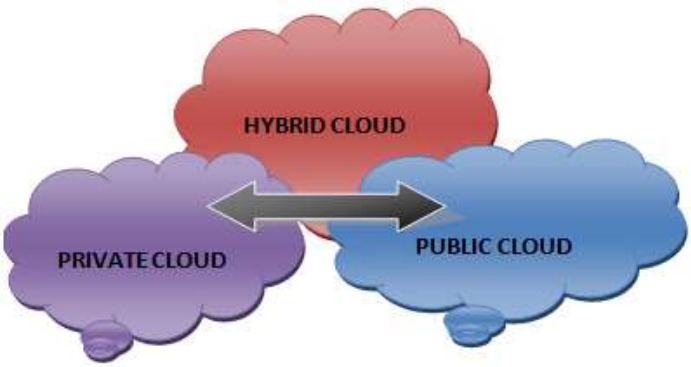

Figure 1: Types of Cloud

The Public Cloud: The term "public" does not always indicate open, even though it can be open or somewhat low-cost to use. A public cloud does not indicate that a user's data is publically observable; public cloud vendor usually provide an entrance manage machine for their users [2].

The Private Cloud: This is a deploy environment within an activity Thus; it must direct its communications alone. In this case, implement a private cloud indicate change the internal communications using technology such as virtualization to deliver services to request, more simply and faster. The advantage of this type of cloud from the public cloud lies in the phase of security and data protection [11].

The Hybrid Cloud: In general, the statement hybrid cloud cohabitation and communication between a private cloud and a public cloud in an organization sharing data and applications

The providers of cloud distinguish three services of cloud computing:

Software as a Service (SaaS)

SaaS software is used straight on the network, with no being downloaded primary in the restricted computer user environments. The software applications are available on the Internet by a SaaS supplier, and are execute in the computing environment predefined from this provider [3]. .

Infrastructure as a Service (IaaS)

IaaS is a absolute computing communications used as a service. To create and use their computing infrastructures freely, according to their needs and only when they need it, users or tenant, admission to specific parts of a consolidate pool of come together property [4].

Platform as a Service (PaaS)

PaaS is a computing surroundings accessible and available, as desired, from an service provider. Used to enlarge and run software [5]. PaaS service providers are to charge for the safety of the stage software stack, and the recommendations during this document are a good basis for ensure a PaaS provider has considered security principles when design and managing their PaaS platform.

In this paper we propose a new approach that Kerberos to make each service secure with the agents. These agents are entities that move from one server to another over the network, with no losing their codes. At each step agents are verified with Kerberos. Authentication is done with the encrypted password. At next stage AS verify the agent. Then user request are forwarded to the TGS. According to the number of requested services TGS generates the number of Kerberos tickets. At next step according to the number of services mobile agents are created and Kerberos tickets are distributed to the mobile agents. Then mobile agents are proceed to cloud layer to execute the task assigning to them.

II. Literature Survey

In the literature there are few works that use mobile agents in the cloud computing:

First we have the work of Priyank et al [6], they propose a trust model based on security agents, which are simple mobile agents that provide security at the virtual machine and the entry point of the network cloud to cloud customers and service providers to manage their resources and data safely and efficiently. These mobile agents not only provide security measures, but also ensured the accounting and monitoring activities in the virtual machine if its malicious or normal state, so that the client is kept informed of the data. If alarming conditions, the client is informed and can take the necessary measures required.

The second architecture is OCCF [7] Cloud Computing Federation (OCCF) is a concept proposed by several researchers, which consists to incorporate and to use several CCSPs (Cloud Computing Service Providers), to provide a uniform resource interface for the clients; the OCCF is based on some notions that can be a good base, to solve the problems of portability and interoperability between the CCSPs. The OCCF is advantageous compared to the other systems, in the following points: Unlimited Scalability, Availability of resources, and Democratization of the Cloud Computing market, Deploying application on multiple CCSPs, and Reduced the cost to the clients. Agents based on Open Cloud Computing Federation (MABOCCF), is a new mechanism that allows the realizing of portability and interoperability, allowing an easy and inexpensive implementation of the OCCF. The experiment results manifests that, the using of MABOCCF optimize the access to the resources over Internet by 50.35% compared with normal systems that don't support the portability between different CCSPs.

In [8] A User Identity Management Protocol for Cloud Computing Paradigm propose user identity management protocol for cloud computing customers and cloud service providers. This protocol will authenticate and authorize customers/providers in other to achieve global security networks. The protocol will be developed to achieve the set global security objectives in cloud computing environments. Confidentiality, integrity and availability are the key challenges of web services' or utility providers. A layered protocol design is proposed for cloud computing systems, the physical, networks and application layer. However, each layer will integrate existing security features such as firewalls, NIDS, NIPS, Anti-DDOS and others to prevent security threats and attacks.

In [9] Applying an Agent-Based User Authentication and Access Control Model for Cloud Servers they offers an agent-based user authentication and access control algorithm based on discretionary and role-based access control model for increasing the reliability and rate of trust in cloud computing environments. The proposed model uses a cloud-based software-as-a-service application with four main agents and a client-based user authentication application. After describing the proposed model, it has been justified and evaluated for identifying the strengths and weaknesses according to defined parameters: Performance, Security, Compatibility, and Power of Intelligence.

In [10] A Study on Security Requirements in Different Cloud Frameworks This paper describes about the different security issues that are occurring in the various cloud computing frameworks and the areas where security lacks and measures can be taken to enhance the security mechanisms.

In[1] Implementation of Cloud Computing Approach Based on Mobile Agents they propose a new approach that uses mobile agents in cloud computing, their architecture is based on mobile agents that have kept the goal of secure communication in cloud computing. In this paper mobile agents are used. At each layer different agents are used for processing the services. In this paper User request services to the interface layer. Mediation layer have two agents i.e. mediator agent and analyzer agent. At mobile agent layer mobile agents are present. The role of each agent is as:

A. Interface layer

1. **Interface agent: -** The primary role of this agent is to only send information from user to the appropriate agents and store this data to the database.

B. Mediation Layer

2. **Mediator agents: -** The role of mediator agents is to act as a mediator between Interface layer and Mediation layer. At mediation layer mediator agent will generate mobile agents to process the service requested from user.

3. **Analyzer agents: -** This agent communicates with mediator agent and analyzes the request of user.

C. Mobile Agent Layer

4. Transfer agents: - These agents are mobile agents and they are generated at mediation layer. They send data to the mediator agents and analyzer agents.

D. Layer Cloud

5. Security agents: - The role of security agents to maintain the security at cloud.

6. Executor agents: - These agents execute the service requested from user. It is a local agent at the cloud, it is responsible for responding to requests from mobile agents arriving at its cloud computing.

III. Proposed Work

This section first presented the objectives of the proposed system, next to objective proposed methodology is presented.

A. The objectives of the system

The main objective of the system is to provide security to the information pass over the cloud. In this system we are using agents to execute the request from the user[9] but we provide here security at each step with AS and TGS.

In this model "mobile agent" means an agent is a process with an completing situation, as well as code and data can move from device to device (called servers) to perform the task assign to it [9] . In this system we authenticate information at each step. A priori, the advantages of mobile agents are various:

I. -The execution of particular agents offer benefit of flexibility more that running a typical process on the server position, and allows communication more forceful than inaccessible communication.

II. - Agents are able to search for information in a smarter way, for example searching by concepts. Agents are also able to correct queries the user, based on the model attached to them.

III. - Agents can create their own knowledge bases that are updated after each search. If the information exchange site, agents are able to find it and next get used to this transform.

IV. - In addition, agents are able to communicate and cooperate with each other (and this is their real strength), which accelerate and facilitate research. If agent is confirmed /authenticate at each layer then unauthenticated user cant request service to the cloud.

III (A). Proposed Methodology / Framework Architecture

The general architecture of our system, shown in Figure

ISSN: 2321-8169
1728 - 1732

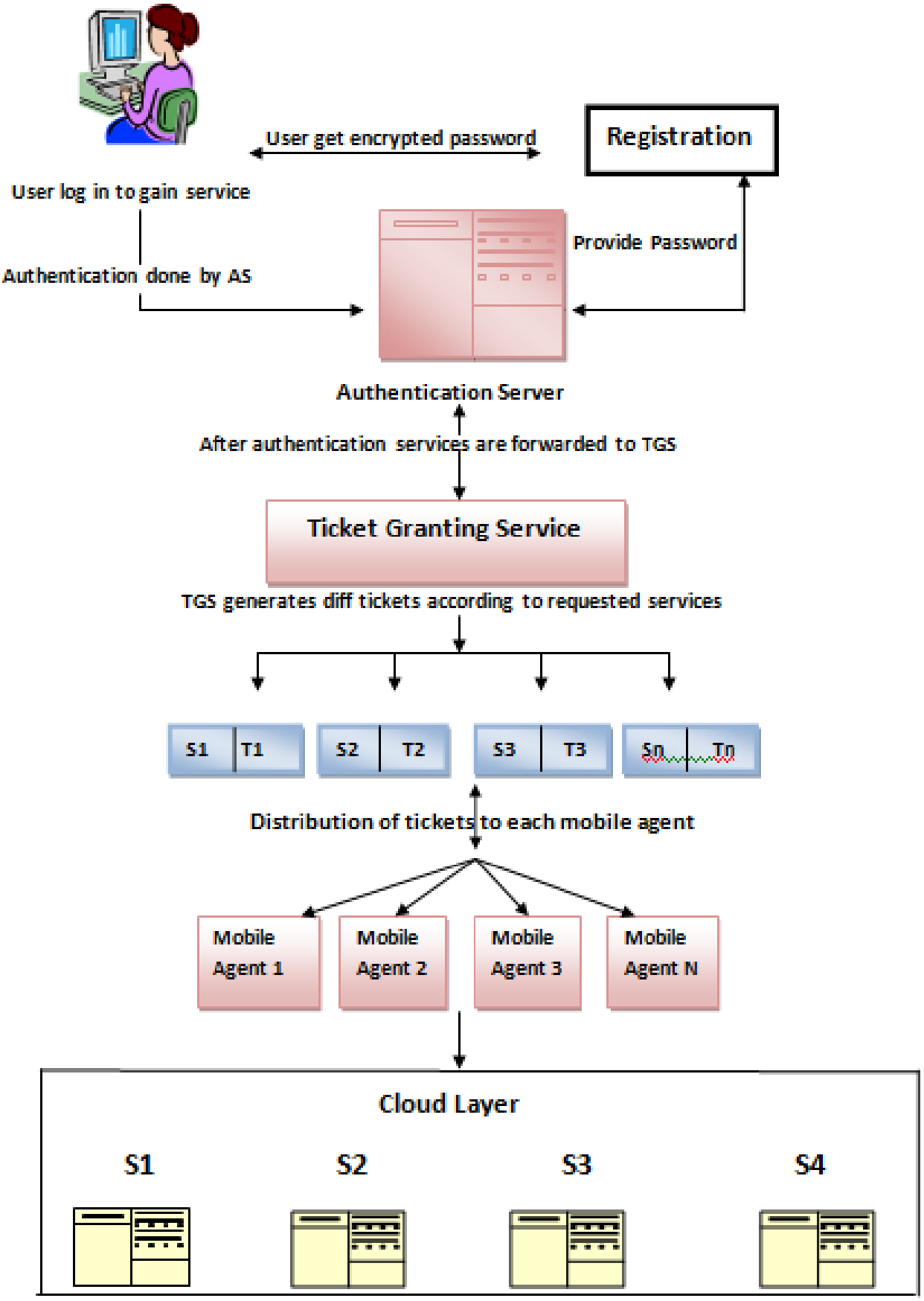

Figure 2: - The Proposed Architecture

AS Layer

User can access this layer with the password provided during registration. User is authenticated by AS at this layer. If he is not registered user, first he must have to registered himself then after he will get encrypted password by AS. Session key will generate with the help of encrypted data and decrypted data. And these session keys are distributed between interface layer and mediation layer.

TGS Layer

In this layer with the help of session keys TGS generates different tickets according to the service requested. After verifying the user at interface layer user can proceed to the mediation layer. At this layer user will get the Kerberos tickets from TGS. After getting tickets it goes to next layer to create mobile agent required for the services requested from the user. This layer generates transfer agents who transfer data to the next layer i.e. mobile agent layer.

Distribution of Tickets

At this layer agents get their services with different tickets. For each service agent will get different ticket. With the help of Kerberos tickets mobile agents are activated to perform service requested by the user. This layer contains all transfer agents generated by the mediation layer. At this level, and for each service request, the mediator agent will activate a set of transfer agents. Each transfer agent will get separate ticket according to the service. After sending all information to the layer cloud they will destroy themselves.

Cloud Layer

At this layer different servers are present in cloud to process the service requested. Each server gets their mobile agent for each service. Mobile agents are distributed for processing the service requests with the help of received tickets from the TGS. At each server mobile agents are distributed as per the service requested from the user. With the help of Kerberos tickets agents will process the service to the correct server according to the service requested from user.

Conclusion

In this research paper, basically cloud data is authentic using authentication servers (AS) hence the information is secured using Kerberos. User can't request service without registration and without encrypted password provided by AS. Also each mobile agent get separate Kerberos tickets for a separate service. So data is transfer with high security provided by Kerberos. In proposed work instead of using different mobile agents for different services, we can use only one mobile agent for all services requested from user therefore with the help of only one mobile agent the time required to generate number of agents for each service will be reduces.

V. References:

[1] Implementation of Cloud Computing Approach Based on Mobile Agents,Alwesabi Ali , Almutewekel Abdullah ,Computer science department, university of Batna, Algeria Batna, Algeria, International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 02– Issue 06, November 2013

[2] A User Identity Management Protocol for Cloud Computing Paradigm, Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3, Lawrence Kehinde

[3] Software-as-a-Service (SaaS) http://www.emc.com/corporate/glossary/software-as-a-service.htm 13 March, 2015.

[4] Infrastructure-as-a-Service (IaaS)http://www.emc.com/corporate/glossary/infrastructure-as-a-service.htm 17 March,2015.

[5] W. Kim, "Cloud Computing: Today and Tomorrow," Journal of Object Technology, vol. 8, no. 1, January-February 2009, pp. 65-72.

[6] Priyank Singh Hada,Ranjita Singh,Mukul Manmohan Meghwal " Security Agents: A Mobile Agent based Trust Model for Cloud Computing" International Journal of Computer Applications (0975 – 8887) Volume 36– No.12, December 2011

[7] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I. Llorente , et al. "The Reservoir model and architecture for open federated cloud computing," IBM Journal of Research and Development, Volume 53, April 2009, in press

[8] A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3, Lawrence Kehinde4

[9] Mostafa Hajivali Faculty of Computer Science Staffordshire University Kuala Lumpur, Malaysia, Maen T. Alrashdan Faculty of Research Coordinator Asia Pacific University (A.P.U.) Kuala Lumpur, Malaysia

[10] Ramandeep Kaur, Pushpendra Kumar Pateriya International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[11] Private cloud, public cloud et hybrid cloud http: //mysaas.fr/2010/10/04/private-cloud-publique-cloud-et-hybrid-cloud/.10 march, 2015.